STATE OF ALABAMA

Information Technology Standard

Standard 670-02S1: Monitoring and Reporting

1. INTRODUCTION:

Changing threat conditions, changes to information systems (including hardware, firmware, software and people), and the potential impact those changes may have on agency operations, assets, or individuals, requires a structured and disciplined process capable of monitoring the effectiveness of the information system security controls on an ongoing basis.

2. OBJECTIVE:

Establish the responsibility for State of Alabama organizations to continuously monitor and report the status of their compliance with State information security requirements.

3. SCOPE:

These requirements apply to all state agencies, boards and commissions with the exception of the Department of Education and the Alabama State Legislature.

4. REQUIREMENTS:

> *Policy: IT Managers shall ensure State of Alabama information systems are continuously monitored in accordance with State standards throughout the system life cycle to provide oversight of information system security controls on an ongoing basis, and status reported to inform the appropriate personnel when changes occur that may impact the security of the system.*

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems, State of Alabama organizations shall perform the following activities to ensure that information security requirements are continuously monitored, documented, and reported:

4.1 SECURITY CONTROL MONITORING

Select an appropriate set of security controls (see Definitions) in the information system to be monitored. Specific threat information, if available, should be used during the system risk assessment to help guide the selection of security controls for the information system.

Continuously monitor the designated controls using methods and procedures selected by the information system owner. Security control monitoring methods may include security reviews, self-assessments, automated tools, security testing and evaluation, or audits.

The IT Manager or senior agency Information Security Officer (ISO) should approve the set of security controls that are to be continuously monitored, and ensure that the security controls (either planned or implemented) for the information system have been documented in the system security plan.

The continuous monitoring of information system security controls shall continue throughout the system life cycle to ensure that important security-related considerations are included in the design, development, implementation, and operation of the information system.

4.2 STATUS REPORTING AND DOCUMENTATION

Update the system security plan based on proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

Create/update a plan of action and milestones that addresses the following:

- Report of progress made on any current or outstanding items listed in the plan
- Vulnerabilities in the information system discovered during security control monitoring
- Describe how the information system owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept the identified vulnerabilities)

The IT Manager or agency ISO shall report the security status of the information system to the State IT Planning, Standards, and Compliance Office. The information in the security status reports (typically conveyed through updated plans of action and milestones) will be used to determine the organization's compliance with State information security standards.

Status reporting should occur at appropriate intervals to transmit significant security-related information about the system, but reports must be updated and submitted at least twice annually or following significant changes affecting system security posture.

4.3 CONFIGURATION MANAGEMENT AND CHANGE CONTROL PROCESSES

NIST Special Publication 800-37 includes configuration management and control as an essential element of the continuous monitoring phase of the system development life cycle.

State of Alabama standards recognize configuration management and change control as a security control common to all State information systems. Configuration management and change control requirements are defined in the applicable policy, standards, and procedures.

5. DEFINITIONS:

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Security controls are defined in NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 670-02: Monitoring and Reporting

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	12/12/2006	